UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/931,487	08/16/2001	Edward W. Kohler JR.	12221-006001	3664

26161 7590 01/14/2009

FISH & RICHARDSON PC
P.O. BOX 1022
MINNEAPOLIS, MN 55440-1022

EXAMINER	
ISMAIL, SHAWKI SAIF	

ART UNIT	PAPER NUMBER
2455	

NOTIFICATION DATE	DELIVERY MODE
01/14/2009	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

PATDOCTC@fr.com

RECORD OF ORAL HEARING

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE BOARD OF PATENT APPEALS

AND INTERFERENCES

Ex Parte EDWARD W. KOHLER, Jr., and MASSIMILIANO A. POLETTO

Appeal 2008-3007
Application 09/931,487
Technology Center 2400

Oral Hearing Held: November 5, 2008

Before HOWARD BLANKENSHIP, JAY P. LUCAS, and THU A. DANG, *Administrative Patent Judges*

APPEARANCES:

ON BEHALF OF THE APPELLANT:

Dennis Maloney, Esquire
FISH & RICHARDSON, P.C.
P.O. BOX 1022
Minneapolis, MN 55440-1022

The above-entitled matter came on for hearing on Wednesday, November 5, 2008, commencing at 9:00 a.m., at The U.S. Patent and Trademark Office, 600 Dulany Street, Alexandria, Virginia, before Dominico Quattrociocchi, Notary Public.

JUDGE BLANKENSHIP: -- hearing and you have 20 minutes and you begin when you like.

MR. MALONEY: Okay. Thank you, very much. This morning I'd like to discuss Claims 1, 2, 4, 6, 9, 11, and 15. All the claims in the application were -- except for Claims 13 and 14 were rejected as anticipated by the Yavatkar and the, and the Claims 13 and 14 which were rejected as being obvious over Yavatkar and Julie Hill (phonetic sp.) I probably will not get to because the Examiner basically uses Hill for a means for classifying attack severity.

Generally, my client's invention is directed to distribute statistical-based techniques for protecting a data center against a denial of service attack. Examiner relies on the Yavatkar's disclosure of watchdog and bloodhound agents. According to the, the reference, a watchdog agent mantra is network traffic and detects an attack and, as a result of that, launches one or more bloodhound agents.

These bloodhound agents traverse nodes in a network to trace the source of the attack, so they jump from node to node. They can either jump to a node or substantiate another bloodhound agent to go to a different node. So this technique requires that the watchdog agent or some other agent determine that there's an attack, and also it requires that that agent determine

what type of attack it is in order to launch a particular type of -- so it's probably only useful if the attack type is known, what type of attack.

In contrast, my client's invention uses data collectors to collect statistical information in packets that are traveling in the network -- and these data collectors are deployed at different points of the network, typically at network peering points as disclosed in the specification -- process that information to determine if there's an attack and, based on the processing of the statistical information, we attempt to find the source of the attack.

Specifically with respect to the claims, Claim 1 includes a novel feature of the action of sending queries to data collectors that are employed at different points in the network, and the data collectors collect the -- information on the network packets sent over the network, and the queries request this statistical information.

And then we also have the feature processing this, this statistical information to determine the source of suspicious network traffic sent to the data center. The Examiner tries to argue that the claim language merely recites sending queries to data collectors to request statistical information and does not specify the type of query. We disagree. We believe that we do specify to take a query because we specify a query for statistical information. Any other requirement or limitation on quote/unquote type of query would only serve to narrow the scope of the claim, and, in view of the Primary Reference, I don't think it's required.

But in any event, we consider that the Yavatkar does not describe this, this technique of sending queries to data collectors for statistical

information. We believe that Yavatkar, if correctly read, does not describe querying of anything or for anything. So that they don't describe the query nor the querying for statistical information.

The -- rather, Yavatkar teaches that this watchdog watches these specific types of bloodhounds. Based on the type of attack, bloodhounds try to trace the attack by traversing from node to node. Our view is not equivalent nor suggests launching -- I'm sorry -- sending the queries to data collectors to try to gather information then process that information based upon using any one of a number of techniques disclosed in the application to determine whether or not the data center is under attack and where the attack is coming from.

JUDGE DANG: Okay, if I may interrupt and ask for a little clarification, it seems the Examiner is trying to -- I, I, guess his finding is that the watchdog directs or commands the bloodhound to do these searches, and then the, the bloodhound then responds by providing reports. So he's saying what's the difference between these commands that, that are given to the bloodhound in order to receive the response? What's the difference between that and query -- and a query?

MR. MALONEY: Well, many differences. First of all, there really is no query of the bloodhound agent. I think we can all agree on that. So the Examiner is basically taking the, the action of launching or substantiating a, a bloodhound agent as being the equivalent of a query; however, the claim specifically talks about sending queries.

In a sense, sending a query, we don't receive just one report which is what Yavatkar -- Yavatkar essentially sends a bloodhound agent to a node.

The node does some processing on that. The bloodhound agent does some processing on that node, looking at the ports and the lengths that traffic is being -- that they're being used in that node, and sends a report back to the watchdog to say these are the ports that had certain types of traffic on it.

JUDGE DANG: Yeah, but --

MR. MALONEY: Any --

JUDGE DANG: But if he sends something back as a response, isn't that a response to a query? I mean, wouldn't, wouldn't this command that requires a response to a query?

MR. MALONEY: No, where is the query?

JUDGE DANG: Well, that's what I'm asking. If a command -- a direction is sent, doesn't that require a response? Isn't that a query?

MR. MALONEY: No. The query, the query come -- in our system --

JUDGE DANG: Okay, yeah, where is the query defined? Do you, do you define the query -- what is a query in your specification that say it is specific? It cannot be a direction that gets a, a response.

MR. MALONEY: Yes, of course we do.

JUDGE DANG: Okay.

MR. MALONEY: In, in -- we -- in the claim, we say sending queries to data collectors. Okay. So we don't, we don't specifically say we send data query to one data collector. We send queries to data collectors, and essentially what happens -- if you could imagine, in that network we have data collectors which are just deployed at different points in that network and the -- if we go back to say a description in the specification we have a

control center or possibly even a gateway sending these queries to different data collectors to try to pinpoint where the attacking traffic is coming from.

And they may be sending -- they'll, they'll likely be sending multiple queries over multiple periods of time to try to figure out where the traffic is coming from. And what they're querying for are not paths that are being taken by these bloodhound agents, but statistical information that's being gathered on the network traffic that's going through those data collectors, and none of that is described in, in Yavatkar. Yavatkar -- all Yavatkar simply does is to try to figure out where -- what links and ports are particularly known, and the network is talking to then try to follow those paths if you will to the next node.

And when they find the node, it then sends a report back to the watchdog saying where, where they found the noded typically they understand the Yavatkar is a little unclear to me, but it seems as though once the watchdog agent -- I'm sorry, the bloodhound agent sends its report to the watchdog agent, it then destroys itself. And the watchdog agent may send out another, another bloodhound agent, or actually the bloodhound agent can also substantiate itself to another node, but there's no transfer back to the watchdog of statistical information. It's all path information, number one, and number two, the watchdog can't later on go and query that data collector for more statistical -- I'm sorry, that bloodhound for more statistical information.

He never queries the bloodhound. He waits for the bloodhound to give him a report back. There's no query that's sent out. Basically, the bloodhound agent does its thing, and when it's finished it sends a report back

to the watchdog, but there's no query, whereas we have a system where we have, you know, likely hundreds or so of data collectors disbursed throughout a large network. I'd hate to find out how large the network is, and we're constantly, you know, sending queries to various data collectors. We may not send them to all of the data collectors as described in the application, but we're trying to pinpoint the traffic. And the difference between the technique that's described in Yavatkar and what's disclosed here is that we don't rely upon the, the known properties of known types of attacks.

Essentially, what we're looking for is irregularities or anomalies in network traffic. We also discuss -- in the specification, we try to compare the statistics to historical information regarding these statistics to try to figure out, you know, where our attacks are coming from and whether or not, in fact, what attack has been launched against the network.

Yavatkar can't -- Yavatkar needs to know what the attack is because they have to send out a particular type of bloodhound agent based upon the attack, and we don't have those limitations. So I think that the technique described in Yavatkar and the technique claimed in our claims is quite different, substantially different.

So again, I don't -- you know, we have a process described in Yavatkar in which the bloodhound agents follow this -- process which it finds a port for the link that's accepting attack traffic on a node in which the, the bloodhound agent is operating. It tries to traverse that link and to move to the node from the other side of the link and then it repeats the process by

the way it moves so the node -- the other side of the link. I guess this is where I'm a little confused in the reference that I believe there is -- it basically launches another bloodhound agent to the other side of that link.

But in any event, that's not what we do. We don't have this thing that moves from link to link trying to figure out where, where the traffic is coming from. We basically just have these data collectors deployed in the network and they -- these things are -- you know, basically they are the network and they get queried by a gateway or a control center when there's -- when people suspect there's an attack going on or even proactively to make sure an attack isn't going on.

And this is not something that's, that's at all suggested by the Yavatkar reference, much less described by the Yavatkar reference. So in Yavatkar everything that Yavatkar does is predicated on the watchdog agent actually detecting the attack or something else actually detecting an attack. So if there's an attack actually going on in the data center that Yavatkar is trying to detect -- trying to protect, but the watchdog and/or the other thing that detects the attack are not capable of doing it, then that could in -- that could make the attack successful because they need to have -- knowledge or knowledge beforehand of the type of attack that's being launched against the data center.

That's not a limitation necessarily in our, our invention. I mean not to say that this invention can detect all possible attacks if some clever attacker would want to launch against the network, but it is clearly not limited to only known types of attacks.

The -- so that's the significant advantages of our scheme over that described in the reference, is that by collecting the statistical information on suspicious packet traffic allows us to detect and stop both known and unknown attacks, and whereas the other reference requires that the -- that something already exists that can recognize the attack.

So with respect to Claim 1, I -- we believe that the features of sending the queries and the features of, of receiving the statistical information and processing that statistical information to determine the source of suspicious network traffic into the data center is neither described nor suggested by the reference.

Claim 2 adds additional feature of, of sending the, the queries to the data collectors for statistical information based on victim destination address. So this obviously is important because in many types of attacks the, the source address of the packet can be spooked. In other words, they're just false addresses. That makes it more difficult to find where the traffic is coming from. However, if you can find data collectors that are receiving -- then more easily pinpoint where the attack is coming from.

And the Examiner tries to -- that because Yavatkar is concerned with gathering information they somehow describes querying gateways based on victim destination address and the -- I just do not see that in the reference, nor do I see that really in any logical construct of the Examiner's argument.

The -- again, what Yavatkar describes is to send reports that detail the path taken during attack, but they don't describe the claim's statistical information and they don't describe getting this information based on attackers that have a destination address for the, for the victim data center.

Claim 4 adds the feature of, of a control center that receives statistical information and further adds the features of sending data to and from the gateway that is associated with the victim data center, and there's no mention in the reference of sending data between a gateway and a control center. The data, as required by Claim 4, has it going to and from the control center, so then it is a situation where the gateway device can also be enlisted to develop some of the statistical information and the control center can, can be processing the statistical information that's coming from the gateway device, again sending queries back and forth. That's not described in the reference.

Claim 6 adds the feature that the queries and the statistical information are sent over a redundant network. The Examiner never really declared where he considers the redundant network. We give, we give -- in our view, what we describe as a redundant network is a network that is physically separated from the network that is actually carrying the traffic. So one of the problems with the techniques described in Yavatkar is that if in fact the network is under a denial of service attack, a serious attack, the network can be so crowded with traffic that in fact the information that is necessary to determine the source of the attack in the reference could never get to the watchdog to actually do anything with it because it could be stuck in the network based upon the volume of traffic being carried by the network -- have a separate network that can carry that traffic, and that's not, that's not addressed at all in Yavatkar.

Claim 9 is directed to the instance in which the source of the attack is behind a gateway and it requires that -- issue a request to the gateway to

prevent the attacking traffic from reaching the network. This, this request is issued by the control center. Yavatkar mentions that if the gateway can be identified it can be shut down, but it doesn't describe any actual way to identify the gateway when the source is behind the gateway. He essentially throws that out as a possibility but doesn't describe actually how to do that. We do describe that.

Claim 11 -- I, I know I'm getting close to my time. I'm just going to try to finish up as quickly as I can. Claim 11 is -- when the source of the attack is not behind a gateway. And when we query the data collectors that are via logically adjacent the gateway to provide information about a possible locations attacking traffic. And again, Yavatkar does not query the -- their bloodhound agents and does not possess a control center so, so cannot meet any of the functionality described in Claim 11.

Finally, 15. Claim 15 up to Claim 1 -- again -- queries the data collectors deployed at different points of the network and the data collectors sample the network pack to collect statistical information and the queries therefore request the statistical information. And again it uses the feature of -- Claim 4 or maybe -- let's see, Claim 2 that the, that the queries are for statistical information from data collectors that examine network traffic with the victim destination address.

So in other words, we can use the data collectors to find out where -- with the victim destination address are going through and query those data collectors as opposed to data collectors that are not seen that, that network traffic and again try to further pinpoint the source of the attack.

And finally I just want to point out to briefly Claim 29 -- scope to -- directed to a computer program product residing on a computer readable medium, and it has the feature of receiving a notification of an attack, and that would typically come from, for example, a gateway that though our victim data center believes it's under attack and that would cause the, the scheme to fall into place and again try to use the querying of the data collectors for statistical information and the processing of the statistical information to try to pinpoint the source of the attack.

So I have basically, you know, went through the claims I went over today. If you have any questions I'd be happy to entertain them.

JUDGE BLANKENSHIP: No, sir, thank you.

MR. MALONEY: Okay, thank you very much.

JUDGE BLANKENSHIP: We're off the record now --

(Whereupon, the hearing concluded at 9:25 a.m. on November 5, 2008.)